United States Senator
BOB BENNETT
Utah

CONTACT: Mary Jane Collipriest, 202-224-5444, Washington, D.C. 20510

FOR IMMEDIATE RELEASE
June 20, 2000

SENATE CLEARS BENNETT-SCHUMER BILL REQUIRING FEDERAL AGENCIES & PENTAGON TO REPORT ON CYBER-DEFENSE PLANS

Coordination necessary to defend against widespread attack, *avert infrastructure collapse*

WASHINGTON, D.C. -- The U.S. Senate has unanimously approved a bill introduced by Sen. Bob Bennett (R-Utah) and Sen. Chuck Schumer (D-NY) requiring that the Department of Defense and all federal agencies report to Congress on their work to counter the global threat of information warfare, a move "critical to ensuring the nation's security in a world of growing cyber threats."

"I cannot overstate my concern for a thoughtful approach to cyber-defense," said Bennett, chairman of the new Senate Critical Infrastructure Protection Working Group. "We have become painfully aware that threats are increasing at unheard-of rates and our defenses, even in the government, have not kept pace."

"This legislation will put our government's cybersecurity planning to the test and it will create a sense of urgency in government agencies that have not made cybersecurity a priority," said Senator Schumer. "We can't wait for an electronic Pearl Harbor to get our cyber defenses in order."

The Bennett-Schumer bill requires the Department of Defense and all Federal agencies to provide Congress with a detailed report of its plans and programs to organize a coordinated defense against attacks on critical infrastructure and critical information based systems in both the public and the private sector.

"One thing my Y2K experience made very clear is that the coordination of intelligence and the proper identification of threat and intention is increasingly difficult. We often lack the human intelligence, just plain people on the ground, to meet the growing need for reconnaissance. This makes coordinated and integrated technology all the more important," said Bennett, who chaired the Senate Y2K Committee.

"Although the United States is far and away the most technologically advanced nation on earth, we are also far and away the most technologically vulnerable. The recent well-publicized hacking and virus incidents cost billions in lost productivity and data and have shown the underlying vulnerabilities of our computer-dependent critical infrastructures to not just lone hackers, but to coordinated

attacks by sophisticated cyber-terrorists who truly mean to do us harm," Schumer added.

The legislation requires that the DoD report to Congress must:

- Describe the role of the DoD in Presidential Decision Directive 63;

- Describe how the DoD is integrating its different capabilities and assets including but not limited too those of the Army's Land Information Warfare Activity (LIWA), the Joint Task Force on Computer Network Defense (JTFCND) and National Communications System into an indications and warning architecture;

- Describe how the DoD is working with the intelligence community to identify, detect and counter the threat of information warfare program of foreign states and transnational organizations;

- Identify the necessary definitions of a "nationally significant cyber-event" and "cyber- reconstitution";

- Describe how DoD is organizing to protect its foreign based infrastructure and networks;

- Identify elements of a defense against an information warfare attack including how the capability of the U.S. Space Command's Computer Network Attack Capability will be integrated into the overall cyber-defense of the U.S.

The legislation also requires that the president must submit a comprehensive report to Congress by July 1, 2001 detailing the specific steps the federal government has taken to develop infrastructure assurance strategies as outlined by Presidential Decision Directive 63 (PDD 63). The report will include the following:

- A detailed summary of the progress of each federal agency in developing an internal information assurance plan.

- The progress of federal agencies in establishing partnerships with relevant private sector industries.

Bennett noted his long-standing concern that Presidential Decision Directive 63 (PDD 63) does not clearly define a role for the Department of Defense (DoD). In one sentence, PDD 63 states that the DoD is assigned the role of 'defense' but does not elaborate on how it will accomplish this vague assignment. The new legislation will require that the DoD begin the thinking process of how the it is integrating its different capabilities and assets into an indications and warning

architecture. "We must begin to work from a position of using the same words for the same things," Bennett said.

The bill was accepted as an amendment to the Department of Defense Authorization Act currently pending in the Senate.

# # #

http://www.senate.gov/~bennett